(19)日本国特許庁（ＪＰ）　(12)**公表特許公報（Ａ）**　(11)特許出願公表番号

特表平10－507324

(43)公表日　平成10年(1998)７月14日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｅ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
		６６０			６６０Ｄ

審査請求　未請求　予備審査請求　有　（全 32 頁）

(21)出願番号　特願平8－509598
(86)(22)出願日　平成７年(1995)９月１日
(85)翻訳文提出日　平成９年(1997)３月５日
(86)国際出願番号　ＰＣＴ／ＵＳ９５／１１１３６
(87)国際公開番号　ＷＯ９６／０８０９２
(87)国際公開日　平成８年(1996)３月14日
(31)優先権主張番号　０８／３０３，０８４
(32)優先日　1994年９月７日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　インテル・コーポレーション
アメリカ合衆国　95052　カリフォルニア州・サンタ　クララ・ミッション　カレッジ　ブーレバード・2200
(72)発明者　デイビス，デレク・エル
アメリカ合衆国・85044・アリゾナ州・フェニックス・イースト　アシァースト　ドライブ・4129
(74)代理人　弁理士　山川　政樹　（外５名）

最終頁に続く

(54)【発明の名称】　ハードウェア・エージェントに対するロビング・ソフトウェア・ライセンス

(57)【要約】
ライセンス供与制限を強制するための集積回路構成要素。前記強制は、ライセンス・プログラムを実行するアクセス特権を集積回路構成要素から他の同様の構成要素に遠隔送信することによって行われる。集積回路構成要素は、固有に指定されたキーの対（１１、１２）、認証装置証明（８０）と、製造業者公開キー（１６）とを暗号アルゴリズムと共に記憶する不揮発性メモリと、集積回路構成要素に入力された情報を処理するために暗号アルゴリズムを実行し、処理された情報を揮発性メモリに送るプロセッサと、固有に指定されたキーの対を集積回路構成要素内で内部的に生成する乱数発生器とを備える。

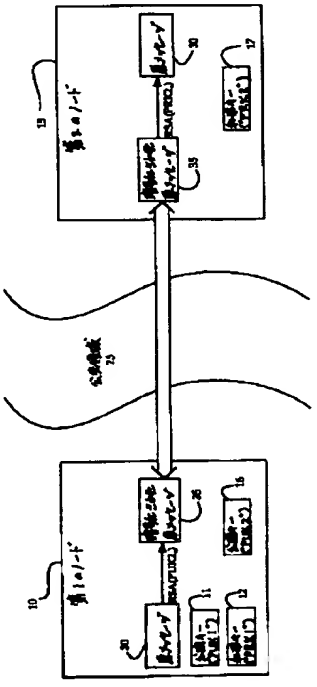

Figure 2

【特許請求の範囲】

１．集積回路構成要素内で情報を処理する処理手段と、

前記処理手段に結合され、集積回路構成要素の製造業者の固有のキー対と認証ディジタル証明と公開キーとを記憶する第１の記憶手段と、

前記処理手段に結合され、前記処理手段によって処理された前記情報を記憶する第２の記憶手段と、

前記処理手段に結合され、前記固有のキー対を生成する手段と、

前記処理手段に結合され、前記集積回路構成要素と第２の集積回路構成要素との間の通信を可能にするインタフェース手段と

を備える前記集積回路構成要素。

２．前記第１の記憶手段が不揮発性メモリを含むことを特徴とする請求項１に記載の集積回路構成要素。

３．前記認証ディジタル証明が、前記製造業者の使用キーによって暗号化された前記集積回路構成要素の前記製造業者の前記公開キーであることを特徴とする請求項２に記載の集積回路構成要素。

４．前記第１の記憶手段が暗号アルゴリズムをさらに含むことを特徴とする請求項２に記載の集積回路構成要素。

５．前記第２の記憶手段がランダム・アクセス・メモリを含むことを特徴とする請求項１に記載の集積回路構成要素。

６．前記生成手段が乱数発生器を含むことを特徴とする請求項５に記載の集積回路構成要素。

７．前記インタフェース手段が、バスに結合されたバス・インタフェースを含み、集積回路構成要素と第２の集積回路構成要素との間に通信リンクを提供して集積回路構成要素が前記第２の集積回路構成要素から集積回路構成要素に送信された情報を復号して記憶し、集積回路構成要素から前記第２の集積回路構成要素に情報を暗号化して送信するようになっていることを特徴とする請求項６に記載の集積回路構成要素。

８．情報の暗号化と復号を行う集積回路構成要素であって、

固有のキー対と、集積回路構成要素の製造業者の装置証明と、前記製造業者の公開キーとを記憶する不揮発性メモリと、

前記情報を記憶するランダム・アクセス・メモリと、

前記不揮発性メモリと前記ランダムアクセスメモリとに結合され、前記情報を内部的に処理する処理装置と、

前記処理装置に結合され、前記固有のキー対を生成する乱数発生器と、

前記処理装置に結合され、集積回路構成要素が少なくとも第2の集積回路構成要素と通信することができるようにするインタフェースと

を備える集積回路構成要素。

9．前記インタフェースが、集積回路構成要素と第2の集積回路構成要素との間に通信リンクを形成して、集積回路構成要素が集積回路構成要素に送信された情報を復号して記憶し、前記集積回路要素から前記第2の集積回路要素に送信される情報を暗号化して送信することができるようにすることを特徴とする請求項8に記載の集積回路構成要素。

10．ソフトウェア・プログラムを実行するホスト処理手段と、

前記ソフトウェア・プログラムを記憶する記憶手段と、

前記ホスト処理手段と前記記憶手段とを結合するバス手段と、

前記バス手段に結合され、エージェント手段に入力された暗号情報を内部的に復号し、前記エージェント手段から出力される暗号情報を内部的に暗号化する前記エージェント手段と

を備えるシステムであって、

前記エージェント手段は、

前記入力暗号情報および出力暗号情報を前記エージェント内で処理する処理手段と、

前記処理手段に結合され、前記入力暗号情報の復号と前記出力暗号情報の暗号化に使用される、固有のキー対と、前記エージェント手段の製造業者の装置証明と、前記製造業者の公開キーとを記憶する第1の記憶手段と、

前記処理手段に結合され、前記入力暗号情報および出力暗号情報を一時的に記憶する第2の記憶手段と、

前記処理手段に結合され、前記固有のキー対を生成する生成手段と、

前記処理手段に結合され、前記システムと遠隔システムとの間の通信を可能にするインタフェース手段と

を含むシステム。

１１．前記第１の記憶手段が、不揮発性メモリから電力が切断されても前記固有のキー対を維持する前記不揮発性メモリを含むことを特徴とする請求項１０に記載のシステム。

１２．前記第１の記憶手段が暗号アルゴリズムをさらに記憶することを特徴とする請求項１１に記載のシステム。

１３．前期生成手段が乱数発生器を含むことを特徴とする請求項１２に記載のシステム。

１４．少なくとも１つの暗号化および復号プログラムを記憶する記憶素子と、

前記暗号化および復号プログラムを実行するホスト・プロセッサと、

前記ホスト・プロセッサと前記記憶素子とを結合するバスと、

前記バスに結合され、内部的に前記遠隔装置からの入力情報を復号し、前記遠隔装置への出力情報を暗号化するハードウェア・エージェントと

を備えるシステムであって、

前記ハードウェア・エージェントは、

前記ハードウェア・エージェント内で前記入力情報と前記出力情報を処理するプロセッサと、

前記プロセッサに結合され、すべてが前記入力情報の復号と前記出力情報の暗号化に使用される、固有に指定されたキー対と、認証装置証明と、製造業者公開キーとを記憶する不揮発性記憶素子と、

前記プロセッサによって処理された前記入力情報と前記出力情報とを一時的に記憶する揮発性記憶素子と、

前記固有のキー対を生成する乱数発生器と、

前記プロセッサに結合され、前記システムと前記遠隔システムとの間の通信を可能にするインタフェースと

を含むシステム。

１５．前記不揮発性記憶素子が少なくとも１つの暗号アルゴリズムをさらに記憶することを特徴とする請求項１４に記載のシステム。

１６．１対のハードウェア・エージェントの遠隔識別と認証のための方法であって、

第1のハードウェア・エージェントと第2のハードウェア・エージェントの間に通信リンクを確立するステップと、

前記第1および第2のハードウェア・エージェントを認証するステップと、

前記第2のハードウェア・エージェントが有効なライセンス・トークンを所有しているか否かを判断するために、前記第1のハードウェア・エージェントから前記第2のハードウェア・エージェントに照会メッセージを送信するステップと、

前記第2のハードウェア・エージェントが前記有効なライセンス・トークンを所有している場合に前記第1のハードウェア・エージェントから第2のエージェントへの転送要求メッセージを生成するステップと、

前記第2のハードウェア・エージェントから前記第1のハードウェア・エージェントに前記有効なライセンス・トークンを転送するステップと、

前記有効ライセンス・トークンを受信した後に前記第1のハードウェア・エージェントから前記第2のハードウェア・エージェントへのトークン受信メッセージを生成するステップと、

前記通信リンクを終了するステップと

を含む方法。

１７．認証ステップが、

前記第1のハードウェア・エージェントに記憶されている固有の装置証明を前記第2のハードウェア・エージェントに送信するステップと、

前記第1のハードウェア・エージェントと通信し前記第1のハードウェア・エージェントを認証するために、前記固有の装置証明を復号して第1のハードウェア・エージェントの公開キーを入手するステップを含むことを特徴とする請求項１６に記載の方法。

１８．認証ステップが、

前記第２のハードウェア・エージェントに記憶されている固有の装置証明を前記第１のハードウェア・エージェントに送信するステップと、

前記第２のハードウェア・エージェントと通信し前記第２のハードウェア・エージェントを認証するために、前記固有の装置証明を復号して第２のハードウェア・エージェントの公開キーを入手するステップとをさらに含む方法。

１９．認証ステップが、

前記第１のハードウェア・エージェントの前記公開キーによって暗号化される呼びかけメッセージを生成するステップと、

前記呼びかけメッセージを前記第２のハードウェア・エージェントに送信するステップと、

前記第２のハードウェア・エージェントが前記呼びかけメッセージを復号し、前記呼びかけメッセージに応答するステップと、

前記第２のハードウェア・エージェントの前記公開キーによって暗号化される呼びかけメッセージを生成するステップと、

前記第１のハードウェア・エージェントに前記呼びかけメッセージを送信するステップと、

前記第１のハードウェア・エージェントが前記呼びかけメッセージを復号し、前記呼びかけメッセージに応答するステップとをさらに含むことを特徴とする請求項１８に記載の方法。

２０．転送要求を生成するステップの前に、

前記第２のハードウェア・エージェントが前記有効なライセンス・トークンを所有しているか否かを前記第２のハードウェア・エージェントが判断するステップと、それによって、

前記第２のハードウェア・エージェントが前記有効なライセンス・トークンを所有していない場合には前記通信を終了するステップと、

前記第２のハードウェア・エージェントが前記有効なライセンス・トークンを所有している場合には前記照会メッセージに対する応答メッセージを生成するステップとをさらに含むことを特徴とする請求項１６に記載の方法。

【発明の詳細な説明】

ハードウェア・エージェントに対するロビング・ソフトウェア・ライセンス

発明の背景

発明の分野

本発明は、ライセンス供与ソフトウェアに関する。詳細には、本発明は、第1のハードウェア・エージェントを有する許可されたノードからライセンス・ソフトウェア・プログラムを実行するアクセス特権を、特定ユーザ・ライセンスに違反することなく第2のハードウェア・エージェントを有する非許可ノードに転送する装置および方法に係わる。

本発明に関する背景技術

コンピュータ・システムの発展の初期には、近代化された企業は一般に、メインフレームに接続されたいくつかの「ダム（ｄｕｍｂ）」端末を有する、一部屋の大きさの集中メインフレームを使用していた。より小型で高速で高性能のコンピュータの登場と共に、それらの近代化された企業の多くは自社の集中メインフレームを撤去して、いくつかのスタンドアロン型コンピュータ、またはパーソナル・コンピュータの集まりを有し、各ユーザが自分のパーソナル・コンピュータを管理する分散ネットワーク（たとえばローカル・エリア・ネットワーク）を使用する方を選んだ。

この非集中化傾向を認めて、多くのソフトウェア開発業者が「ユーザ特有の」ライセンスと一般に呼ばれる特定のライセンス供与方式に従って自社のソフトウェアをライセンス供与している。ユーザ特有のライセンスは一般に、特定のソフトウェア・プログラムを特定の方式で随時操作することを所定数の個人に許可する。したがって、ライセンスは特定のノードではなく選択された数の個人に付随する。本出願の範囲では、「ノード」とは、好ましくは本発明を含む、コンピュータ、プリンタ、ファクシミリ機、および同様のものなどの「インテリジェンス」を有するハードウェア製品であると定義する。ユーザ特有のソフトウェアに付随する主要な問題は、ソフトウェア開発業者の潜在的ライセンス供与収益をむしばむライセンス・ソフトウェアの無許可の使用またはコピーあるいはその両方を

間接的に助長することてある。

長年にわたり、ソフトウェア開発業者は、自社のソフトウェアがユーザ特有のライセンスの条件の範囲を超えて使用およびコピーされないように保護する方法を探し求めてきたが、企業ライセンス被供与者は自社の従業員によるライセンス・ソフトウェアの不法な使用またはコピーによる潜在的な代位責任を大幅に軽くしようとしてきた。したがって、ユーザ特有のライセンスの条件を超えたソフトウェアの拡散を防止することは、ソフトウェア開発業者と企業ライセンス非供与者の両方に同様に利益がある。

現在、ユーザ特有のソフトウェア・ライセンスの遵守は、「ドングル（ｄｏｎｇｌｅ）」と呼ばれる物理的ハードウェア装置の使用によって行われている。ドングルとは、最初に購入したときにライセンス・ソフトウェアと共にパッケージされている物理ハードウェア装置である。これは一般には、たとえばパーソナル・コンピュータなどのノードのパラレル・ポートに接続する。実行中の様々な時点で、対象ライセンス・ソフトウェア・プログラムはドングル内で使用されているアクティブ装置に許可メッセージ（「呼びかけ」と呼ばれる）を送る。ドングル内のアクティブ装置は、ドングル内部に記憶されている秘密情報（以下、「有効ライセンス・トークン」と呼ぶ）を使用してその呼びかけを処理し、戻りメッセージ（「応答」と呼ぶ）を発生する。ソフトウェア・プログラムはこの応答を期待応答と比較し、その２つの応答が同じである場合にのみそれ以降の実行を許可する。

したがって、ユーザはライセンス・ソフトウェア・プログラムをコピーし、それを複数のパーソナル・コンピュータにロードすることはできるが、そのソフトウェア・プログラムを実行することができるのはドングルが接続されている第１のコンピュータのみである。ライセンス・ソフトウェア・プログラムを他のパーソナル・コンピュータで実行するためには、第１のパーソナル・コンピュータからドングルを取り外して他のパーソナル・コンピュータに接続しなければならない。その結果、第１のパーソナル・コンピュータではそのソフトウェアは使用不能になる。企業ライセンス被供与者に与えられるドングルの数は一般にユーザ特

有のソフトウェア・ライセンス契約を結んだ人数に限定されているため、ライセンス・ソフトウェア・プログラムの複数の導入がソフトウェア開発業者にとって不利な財務上の影響を引き起こさないことは明らかである。

ドングルによってユーザ特有のライセンスの遵守は確保されるが、いくつかの欠点がある。１つの欠点は、ドングルを顧客に物理的に配布しなければならないことである。したがって、ソフトウェアの電子配布用システム（「コンテンツ配布」と呼ぶ）が提案され、実施されて便利さを増し、配布コストを削減しているが、物理装置としてのドングルは依然として従来の配布方法とそれに伴う費用とを必要とする。ソフトウェア開発業者の経済的利益を保護するためにドングルを必要とすることによって、顧客は、（ｉ）選定された場所でドングルを直接入手し、その後でそのドングルをノードに装着してからでなければライセンス・プログラムを使用することができないか、または（ii）意図した使用の前にコンテンツ配布者が顧客にドングルを郵送する時間を見越してライセンス・ソフトウエア・プログラムを発注するという煩わしい作業に耐えなければならない。いずれにしても、ドングルはコンテンツ配布の効率と興味を妨げる。

もう一の欠点は、ドングルの取り外しと装着が時間のかかる処理であることである。時間を争う企業では、ドングルの交換は企業の業績全体に影響を及ぼす。他の欠点は、ドングルを絶えず取り外したり装着したりすることによって、ドングルが損傷し機能不能になる確率が高くなり、企業は新しいドングルを待ってからでなければ、そのソフトウェア・アプリケーションを再び使用することができない。

他の欠点は、ライセンスは個人を対象としているが、ドングルは一般にノードに装着されることである。したがって、ユーザが別の機械（たとえば自宅にあるパーソナル・コンピュータ）に移動した場合、そのユーザはドングルを所有していない限り、ライセンス・ソフトウェア・プログラムを使用することができない。

発明の簡単な概要

上記に基づき、ノード内に内部実装された集積回路構成要素として、電子ドン

グルの機能を備えた暗号装置を作製することが望ましい。したがって、本発明の目的は、集積回路構成要素を遠隔認証する際に使用する固有ディジタル証明を内部的に記憶する記憶素子を備えた、集積回路構成要素としての暗号装置を提供することである。

本発明の他の目的は、固有の公開キーと私用キーとの対を内部的に生成し、少なくとも秘密キーを記憶することができ、それによって集積回路構成要素の外部の使用を防止する固有集積回路構成要素を提供することである。

本発明の他の目的は、あるエンティティによって検証または製造された別の同様の集積回路構成要素とのセキュリティ保護された通信を可能にするために、そのエンティティの公開キーを内部的に記憶する集積回路構成要素を提供することである。

本発明の他の目的は、ハードウェアの物理的操作を頻繁に必要としないロビング（ｒｏｖｉｎｇ）・ソフトウェア・ライセンスを与える集積回路構成要素を提供することである。

この集積回路構成要素を一般にハードウェア・ライセンスと呼び、識別のための動作を行う処理装置と、（ｉ）固有の公開キーと私用キーの対を記憶する不揮発性メモリと、（ii）キーの対が認証されたものであるかどうかを検証するディジタル証明と、（iii）集積回路構成要素と製造業者によって製造された他の同様の構成要素との間の通信を可能にする選定されたエンティティ（集積回路構成要素の製造業者であることが好ましい）の公開キーとを含む記憶素子を備える。不揮発性メモリは暗号アルゴリズムを記憶するためにも使用することができる。集積回路構成要素は、処理装置によって処理される情報を記憶する揮発性メモリと、他の同様の構成要素から通信バスを介して暗号化形式または復号形式の情報を送受信するためのインタフェースと、固有の公開キーと私用キーの対を生成するための乱数発生器とをさらに備える。

図面の簡単な説明

本発明の目的、特徴、および利点は以下の本発明の詳細な説明を読めば明らかになろう。

第1 図は、双方向対称キー暗号化および復号プロセスを示すブロック図である。

第2 図は、双方向非対称キー暗号化および復号プロセスを示すブロック図である。

第3 図は、信用権威者からのディジタル証明プロセスを示すブロック図である。

第4 図は、本発明の実施形態を組み込んだコンピュータ・システムのブロック図である。

第5 図は、本発明の実施形態を示すブロック図である。

第6 図は、対とディジタル証明を集積回路構成要素に実装する方法を示すフローチャートである。

第7 Ａ図～第7 Ｃ図は、ライセンス特権を有する第2 のハードウェア・エージェントと第1 のハードウェア・エージェントとの間で有効ライセンス・トークンを転送するために、第1 のハードウェア・エージェントが第2 のハードウェア・エージェントとの通信を確立する操作を示すフローチャートである。

発明の詳細な説明

本発明は、適切に構成されたハードウェア・エージェント間でロビング・ソフトウェア・ライセンスを転送することができるようにし、それによって配布する物理ハードウェア装置を不要にする装置および方法に関する。以下の説明では、本発明を十分に理解することができるように多くの詳細を記載する。しかし、当業者には、本発明の精神および範囲から逸脱することなく、本発明を例示されているものとは異なる多くの実施形態を使用して実施することができることが明らかである。他の場合には、本発明を無用に不明瞭にしないために、周知の回路、要素、および同様のものについては詳細には記載しない。

詳細な説明では、特定の特性または品質を説明するためにいくつかの暗号関係の用語を頻繁に使用するが、ここでそれらについて定義する。「キー」とは従来の暗号アルゴリズムの暗号化または復号あるいはその両方のパラメータである。具体的には、キーはn ビットの長さの二進データの順次配置（「ストリング」）

である（ただし「ｎ」は任意の数である）。「メッセージ」とは、一連のバス・サイクルで転送される情報（たとえば暗号化キー・アドレスおよびデータ）であると一般に定義される。この情報には、呼びかけや戻り応答が含まれる。「ディジタル証明」とは、通信を開始するエンティティに関係する情報であると定義され、典型的には広く公開された信用権威者（たとえば銀行、政府機関、同業組合など）によって私用キーを使用して暗号化されたエンティティの公開キーである。「ディジタル署名」とは、ディジタル証明と類似しているが、送信者ではなくメッセージ自体の認証に使用される。

ここ数年、１つの場所から他の場所にディジタル情報を送信することがますます望まれるようになっている。その結果、現在、多くのエンティティが暗号技術を使用しており、それによって正当な受信者にとっては明瞭であいまいさがないが不正な受信者には理解できない方式で情報が転送される。一般に、暗号技術は２つの従来の技法のうちの１つに従って機能する。すなわち、対称キー暗号化または非対称（または公開）キー暗号化あるいはそれらの暗号化技術の組合せである。

第１図を参照すると、対称キー暗号技法の実施形態が図示されている。この技法では、同一、すなわち対称な秘密キー（「ＳＫ」と符号が付されている）１を使用して、第１のノード１０と第２のノード１５の間で転送される原メッセージ５を暗号化して暗号化された原メッセージ２０を形成し、暗号化された原メッセージ２０を復号して原メッセージ５を復元する必要がある。このような暗号化および復号は、たとえばデータ暗号アルゴリズム（より一般には「ＤＥＳ」と呼ばれる）などの周知の従来の暗号アルゴリズムを使用して行われる。原メッセージ５は、（ｉ）第１のノード１０で暗号化され、（ii）電話回線および同様のものなどの公共領域２５を使用して第１のノード１０から第２のノード１５に転送され、（iii）第２のノード１５で復号される。しかし、この技法は秘密キー（「ＳＫ」）を前もって設定する必要があるため、ユーザ数が多い場合にはサポートするのが困難である。

次に第２図を参照すると、非対称キー技法の実施形態が図示されている。この技法は、暗号化と復号に別々に使用される２つの別々のキー（「公開キー」およ

び「私用キー」と呼ぶ）を使用する。第１のノード１０から第２のノード１５への双方向通信を確立するために、第２のノード１５のキーの対のうちの「公開」キー１６（「ＰＵＫ２」と符号が付されている）が第１のノード１０に記憶され、一般に第１のノード１０が暗号化の分野で周知の非対称「ＲＳＡ」アルゴリズムに基づいて原メッセージ３０を暗号化するために使用する。これによって、第２のノード１５に転送される暗号化原メッセージ３５が形成される。第１のノード１０の公開キーと私用キーの対１１および１２（［ＰＵＫ１」および「ＰＲＫ１」と符号が付されている）はさらに第１のノード１０に記憶される。

第２のノード１５のキーの対のうちの「私用」キー１７（「ＰＲＫ２」と符号が付されている）は、第２のノード１５のみが知っており、第２図に示すようにＲＳＡアルゴリズムに基づく第１のノード１０からの暗号化メッセージ３５の復号を含む多くの目的のために使用する。しかし、この技法は、不正なエンティティ（たとえば商業スパイなど）が正当なエンティティ（たとえば従業員、合弁企業など）を装おって、仕事の流れを中断させたり機密情報を入手したりするために他の正当なエンティティに詐欺的メッセージを送信しようとする試みを許しやすい。したがって、一般に付加的なプロトコルを使用して、メッセージの認証を行い、そのメッセージを送信するエンティティの正当化を行う。

事前には未知である当事者間で最初に通信を確立するときは、送信者の認証（すなわち公開キーの送信者が実際にその公開キーの真の所有者であることの検証）が問題である。この問題は、一般に、送信メッセージ５０内にディジタル証明４５を組み込むことによって回避される。ディジタル証明４５は、相互信用権威者５５（たとえば銀行、政府機関、同業者組合など）が、署名文（「ＳＭ」と符号が付されている）５８を使用して通信を開始するノードの公開キー（「ＰＵＫ１」）１１を、信用権威者５５の私用キー（「ＰＲＫＴＡ」）５７を使用して暗号化することによって発行する。したがって、ＰＵＫ２　１６を使用しようとする不正な試みが行われてもその送信メッセージに対しては受信者には読めない応答が返されることになるだけてある。選択される信用権威者５５は、関係当事者によって異なる。たとえば、同じ企業に雇用されている２人の個人は両者とも、その企業の会社セキュリティ管理局によって発行された証明を信用する。しかし

、

２つの独立した企業エンティティの従業員は、それぞれのセキュリティ管理局からの認証だけでなく、たとえばそのような企業エンティティを証明する何らかの産業組織からの証明も必要とする。

この手法では、複数の操作を並列して実行して送信メッセージ５０を作成する。１つの操作は、ＤＥＳアルゴリズムを介して対称秘密キー（「ＳＫ」）６０を使用して原メッセージ４０を暗号化して、ディジタル証明４５と共に送信メッセージ５０に入れられる暗号化メッセージ６５を形成することである。原メッセージ４０にはハッシュ・アルゴリズム７０（たとえば「ＭＤ５」）も適用されて、送信メッセージ・ダイジェスト７５が形成される。送信メッセージ・ダイジエスト７５は、第1のノードの私用キー（「ＰＲＫ１」）１２を使用してさらに暗号化されてディジタル署名８０を形成し、それが送信メッセージ５０に入れられる。さらに、対称キー（「ＳＫ」）６０がＲＳＡアルゴリズムに基づいて第2のノードの公開キー（「ＰＵＫ２」）１６を使用して暗号化されて「ＳＫｅｎｃ」８５となり、さらに送信メッセージ５０に入れられる。

第3図を続けて参照する。第1のノード１０から公共領域２５を介して送信される送信メッセージ５０を受信すると、第2のノード１５は私用キー（ＰＲＫ２」）１７を使用してＳＫｅｎｃ８５を復号し、信用権威者５５の発行公開キー（「ＰＵＢＴＡ」）を使用してディジタル証明４５を復号し、ＳＫ６０とＰＵＫ１１を入手する。このＳＫキー６０とＰＵＫ１キー１１を使用して、暗号化原メッセージ６５とディジタル署名８０を復号し、送信メッセージ・ダイジェスト７５と原メッセージ４０をそれぞれ取り出す。次に、原メッセージ４０に第1のノード１０で行われたのと同じハッシュ・アルゴリズム８５を適用する。その結果９０（「受信メッセージ・ダイジェスト」と称する）が、送信メッセージ・ダイジェスト７５と比較される。送信メッセージ・ダイジエスト７５が受信メッセージ・ダイジェスト９０と同じ場合、この2つの正当ノード間の通信が維持される。

第4図を参照すると、本発明を使用するコンピュータ・システム１００の実施

形態が図示されている。コンピュータ・システム１００は、ホスト・プロセッサ１０５と、メモリ装置１１０と、入出力（「Ｉ／Ｏ」）制御装置１１５と、「ハードウェア・エージェント」と呼ばれる暗号装置１２とを備える。複数のバス・エージェントがシステム・バス１３０を介して互いに接続され、それによってこれらのバス・エージェント間で情報を伝達することができる。

この実施形態ではホスト・プロセッサ１０５しか図示されていないが、コンピュータ業界では周知のように、コンピュータ・システム１００内で複数のホスト・プロセッサを使用することもできるものと企図される。さらに、メモリ装置１１０はダイナミック・ランダム・アクセス・メモリ（「ＤＲＡＭ」）、読取り専用メモリ（「ＲＯＭ」）、ビデオ・ランダム・アクセス・メモリ（「ＶＲＡＭ」）、および同様のものを含むことができる。メモリ装置１１０には、ホスト・プロセッサ１０５が使用する情報が記憶される。

入出力制御措置１１５は、入出力バス１３５とシステム・バス１３０との間のインタフェースであり、システム・バス１３０または入出力バス１３５に結合された構成要素間で情報を転送する通信経路（すなわちゲートウェイ）を提供する。入出力バス１３５はコンピュータ・システム１００内の少なくとも１つの周辺装置との間で情報を転送する。これには、画像を表示する表示装置１４０（たとえば陰極線管、液晶表示装置など）、ホスト・プロセッサ１０５に情報およびコマンド選択を伝達する英数字入力装置１４５（たとえば英数字キーボードなど）、カーソル移動を制御するカーソル制御装置１５０（たとえばマウス、トラックボール、タッチ・パッドなど）、情報を記憶する大容量データ記憶装置１５５（たとえば磁気テープ、ハード・ディスク・ドライブ、フロッピィ・ディスク・ドライブなど）、コンピュータ・システム１００から他の装置に情報を送信する情報送受信装置１６０（ファックス機、モデム、スキャナなど）、および情報の有形の視覚表現を提供するハード・コピー装置１６５（たとえばプロッタ、プリンタなど）が含まれるがこれらには限定されない。第4図に示すコンピュータ・システムはこれらの構成要素または例示したもの以外の構成要素のうちの一部または全部を使用することができる。

次に、第5図に示す本発明の実施形態を参照すると、ハードウェア・エージェント１２０は、ホスト・プロセッサ１０５および、メモリおよび入出力制御装置（図示せず）との通信経路を確立するシステム・バス１３０に結合されている。ハードウェア・エージェント１２０は、ダイ１２１を損傷と有害汚染物質から保護するように集積回路構成要素パッケージ１２２内に、好ましくは密閉されてカプセル封止されたダイ１２１（たとえばマイクロコントローラ）の形態の単一の集積回路を含む。ダイ１２１は、記憶素子１２４に結合された処理装置１２３と、バス・インタフェース１２５と、乱数発生器１２６とを含む。バス・インタフェース１２５は、ハードウェア・エージェント１２０から他の装置（たとえばホスト・プロセッサ、他の装置内の他のハードウェア・エージェントなど）への通信を可能にする。処理装置１２３は、ダイ１２１の中のセキュリティ保護された環境内で内部的に計算を行って、許可された受信者との有効な接続を確認する。そのような計算には、特定のアルゴリズムおよびプロトコルの実行、装置固有の公開／私用キー対および同様のものを生成する、回路（たとえばランダムな性質であることが好ましい、乱数発生器１２６など）の起動が含まれる。処理装置１２３は、コンピュータ・システムを混乱させてその私用キーおよびその他の情報を入手する一般的な方法であるウィルス攻撃による私用キーのアクセスを防ぐようにダイ１２１内に配置されている。

記憶素子１２４は、「ＲＳＡ」や「ＤＥＳ」などの適切な暗号アルゴリズム、公開キーと私用キーの対１２７ａ、価値の対が認証されたものであるかどうかを検証するためのディジタル証明（「ＤＣ」という符号が付されている）１２７ｂ、および集積回路構成要素とその製造業者によって製造された他の同様の装置との間の通信を可能にする集積回路構成要素の製造業者の公開キー（「ＰＵＫＭ」）１２７ｃを記憶するフラッシュ・メモリなどの不揮発性メモリ素子１２７を含む（第6図に詳細に記載する）。電源が切断されても内容を保持するため、この不揮発性メモリ１２７が主として使用される。メモリ装置１２４は、処理装置１２３からの特定の結果を記憶するためにさらにランダム・アクセス・メモリ（「ＲＡＭ」）１２８を含む。

ハードウェア・エージェント１２０は、セキュリティ強化のためにシステム・バス１３０に接続された周辺装置として実装されているが、ハードウェア・エージェント１２０はＰＣプラットフォーム・レベルで他のいくつかの方法（たとえば、ハード・ディスクから入出力される情報の自動的な復号または暗号化あるいはその両方を行うディスク制御装置またはＰＣＭＣＩＡカードとしてなど）で実施することもできるものと企図される。他の代替実施態様は、後述するようにハードウェア・エージェントをホスト・プロセッサを含むマルチチップ・モジュールの１つの構成要素とすることであろう。さらに、ハードウェア・エージェントについてＰＣプラットフォームと関連して説明しているが、このようなハードウェア・エージェントはファックス機、プリンタおよび同様のものなどのノード内や、コンピュータと入出力周辺装置との間の通信経路上に実施することもできるものと企図される。

第6図を参照すると、本発明を製作する操作のフローチャートが示されている。まず、ステップ１００で、任意の従来の公知の半導体製造技法に従ってハードウェア・エージェントのダイを製作する。次に、ハードウェア・エージェント自体を形成するようにそのダイを半導体パッケージ内にカプセル封止する（ステップ１０５）。証明システム上にハードウェア・エージェントを配置し、それによってハードウェア・エージェントと証明システムとの間に電気的および機械的結合を確立する（ステップ１１０）。証明システムは、ハードウェア・エージェントの証明のための電気信号の発生と受信を行う、プリント回路基板に結合されたキャリヤを備える。証明システムはさらに、固有キー生成を保証するために前に生成された公開キーの記憶装置（たとえばデータベース）をさらに備える。その後で、証明システムはハードウェア・エージェントに電力を供給し、ハードウェア・エージェントは乱数発生器に電力を供給してハードウェア・エージェント内で乱数発生器が装置固有の公開キーと私用キーの対を内部的に生成することができるようにする。

ハードウェア・エージェント内で公開キーと私用キーの対が生成された後、公開キーと私用キーの対のうちの公開キーを証明システムに送る（ステップ１２０

）。その公開キーを、記憶装置に記憶されている前に製造されたハードウェア・エージェントの前に生成された公開キーと比較する（ステップ１２５）。万一、その公開キーが前に生成された公開キーの１つと同じである場合（ステップ１３０）、証明システムがハードウェア・エージェントに対して別の前記公開キーと私用キーの対を生成するように通知し（ステップ１３５）、このプロセスをステップ１２０から続けて各公開キーと私用キーの対が確実に固有のものになるようにする。

公開キーが固有である場合は、記憶装置はその固有の公開キーで更新される（ステップ１４０）。その後、証明システムがステップ１４５で、キーの対が認証されたものであるかどうかを検証する固有装置証明（以下、「認証装置証明」と呼ぶ）を作成する。認証装置証明は、秘密私用製造業者キーを使用して「ディジタル署名」された装置の公開キーを少なくとも含む（すなわち、大ざっぱに言えば製造業者の私用キーを使用して装置の公開キーを暗号化する）。この認証装置証明を製造業者の一般に知られた公開キーと共にハードウェア・エージェントに入力し（ステップ１５０）、ハードウェア・エージェントは固有公開キーと私用キーの対と認証装置証明と製造業者の公開キーをその不揮発性メモリに永久的にプログラムする（ステップ１５５）。しかし、製造業者の代わりに他のエンティティ（たとえば配布業者）の公開キーを使用することもでき、その場合は認証装置証明の変更も必要になることが企図される。この時点で、ハードウェア・エージェントは物理的に固有であり、これで他のハードウェア・エージェントとの通信を安全に確立することができる。

ハードウェア・エージェントを製作した後、それを第4図に示すコンピュータ・システムなどの電子装置に実装する。これは、呼びかけ／応答などの認証手続きとその他の周知の手続きを使用してライセンス供与者とハードウェア・エージェントとの間にセキュリティ保護された通信経路を確立することによって行うことができる。通信経路が安全に確保された後、セキュリティ保護された通信リンクを介して有効なライセンス・トークンをハードウェア・エージェントのフラッシュ・メモリにダウンロードする。ハードウェア・エージェント間で転送するの

ではなく、ライセンス・トークンが複数のハードウェア・エージェントに組み込まれて「有効」状態または「無効」状態にあり、それによってライセンス・トークンを有効化または無効化することもできることがさらに企図される。

第７Ａ図および第７Ｂ図を参照すると、２つのハードウェア・エージェントの認証の相互遠隔識別の実施形態が示されている。ステップ２００で、第１のハードウェア・エージェントが組み込まれた「未許可の」第１のノード（すなわち現在はライセンス・ソフトウェア・アプリケーションの操作を許可されていないノード）と、ライセンス・ソフトウェア・アプリケーションを操作することを許可

された第２のハードウェア・エージェントが組み込まれた許可された第２のノードとの間に通信リンクが確立される。この通信リンクは、モデム、ネットワークなどの任意の従来の通信手段を介して確立することができる。第１のハードウェア・エージェントはその固有認証装置証明を含むメッセージを第２のハードウェア・エージェントに出力する（ステップ２０５）。両方のハードウェア・エージェントの不揮発性メモリに製造業者の公開キー（「ＰＵＫＭ」）がプログラムされているため、第２のハードウェア・エージェントは製造業者の公開キー（「ＰＵＫＭ」）を使用して認証装置証明を復号し、第１のハードウェア・エージェントの公開キーを入手する（ステップ２１０）。その後、ステップ２１５～２２０で、ステップ２０５～２１０に記載されているものと同様の操作も行われ、それによって第１のエージェントは第２のハードウェア・エージェントの公開キー（「ＰＵＫ２」）を入手する。

その後、ステップ２２５および２３０で、第２のハードウェア・エージェントが、第１のハードウェア・エージェントの導き出された公開キーを使用して、選定された暗号アルゴリズム（たとえばＲＳＡ）に従って呼びかけメッセージを暗号化し、その呼びかけメッセージを第１のハードウェア・エージェントに送信する。ステップ２３５および２４０で、第１のハードウェア・エージェントが、その私用キー（「ＰＲＫ１」）を使用して呼びかけメッセージを復号し、次に、復号した呼びかけメッセージを第２のハードウェア・エージェントの公開キー（「ＰＵＫ２」）を使用して暗号化することによって応答メッセージを生成し、その

応答メッセージを第２のハードウェア・エージェントに送信する。次に、第２のハードウェア・エージェントが、前に送信された製造業者の装置証明の復号によって前に判断したその私用キー（「ＰＵＫ１」）を使用してその応答を復号する（ステップ２４５）。ステップ２５０で、第２のハードウェア・エージェントは元の呼びかけメッセージを、復号した応答メッセージと比較し、同じでない場合は通信を終了する（ステップ２５５）。同じ場合は、ステップ２６０～２９０でステップ２２５～２６０と同様の呼びかけ／応答手続きが行われて、第１のハードウェア・エージェントから送信された情報を第２のハードウェア・エージェントが実際に受信していることを検証する。これらのステップ（ステップ２２５～２９０）が成功裏に完了すると、両方のハードウェア・エージェントが認証されたエージェントであり、両者の間の通信がセキュリティ保護されていることが保証される（ステップ２９５）。

次に第７Ｃ図を参照すると、セキュリティ保護された通信のもとで第２のハードウェア・エージェント内の有効なライセンス・トークンを第１のハードウェア・エージェントに安全に転送するプロセスの実施形態が示されている。安全保護された通信が確立されると、第１のハードウェア・エージェントは第２のハードウェア・エージェントに対して有効なライセンス・トークンを所有しているかどうか照会する（ステップ３００）。第２のハードウェア・エージェントが組み込まれているシステムが有効なライセンス・トークンを持っていない場合（ステップ３０５）、ハードウェア・エージェント間の通信は終了する（ステップ３１０）。しかし、第２のハードウェア・エージェントが組み込まれたシステムが有効なライセンス・トークンを持っている場合は、第１のハードウェア・エージェントにしかるべくメッセージを送信する（ステップ３１５）。

第１のハードウェア・エージェントは、このメッセージを受信すると、第１のハードウェア・エージェントにライセンス・ソフトウェア・アプリケーションの操作を許す有効なライセンス・トークンの転送要求を出す（ステップ３２０）。第２のハードウェア・エージェントは、有効なライセンス・トークンを転送することによって転送要求に応答し、それによってそのライセンス特権を失う（ステ

ップ３２５）。第１のハードウェア・エージェントはその有効なライセンス・トークンを受け取り、そのトークンをその不揮発性メモリに記憶した後、有効なライセンス・トークンを受け取ったというメッセージを第２のハードウェア・エージェントに送信し、そのライセンス・ソフトウェアのコピーを使用可能にすることになる（ステップ３３０）。この時点で、通信が終了する（ステップ３３５）。

ステップ３２０と３２５の間およびステップ３２５と３３０の間に呼びかけ／応答シーケンスを導入することによって、追加のレベルのプロトコル保全性を得ることができることが企図される。これによって、前のライセンス・トークン転送事象の「再生」が防止される。

第１と第２のハードウェア・エージェント間の通信と並行して、各ハードウェア・エージェントはその送信の内容を監査ログとして不揮発性メモリに記憶する。したがって、第２のハードウェア・エージェントがそのコピーを使用不能にした後で第１のハードウェア・エージェントがそのコピーを使用可能にする前に通信が切断された場合、両方のハードウェア・エージェントは通信が再接続された後で監査ログを見直してどのハードウェア・エージェント（ある場合）がライセンス・ソフトウェア・アプリケーションを操作する許可を持っているかを判断することができる。

本明細書に記載の本発明は多くの異なる方法で多くの異なる構成を使用して設計することができる。本発明について様々な実施態様に関して説明したが、当業者なら本発明の精神および範囲から逸脱することなく他の実施態様を考えつくであろう。したがって、本発明は請求の範囲の記載によって判断されるべきである。

【 図１ 】

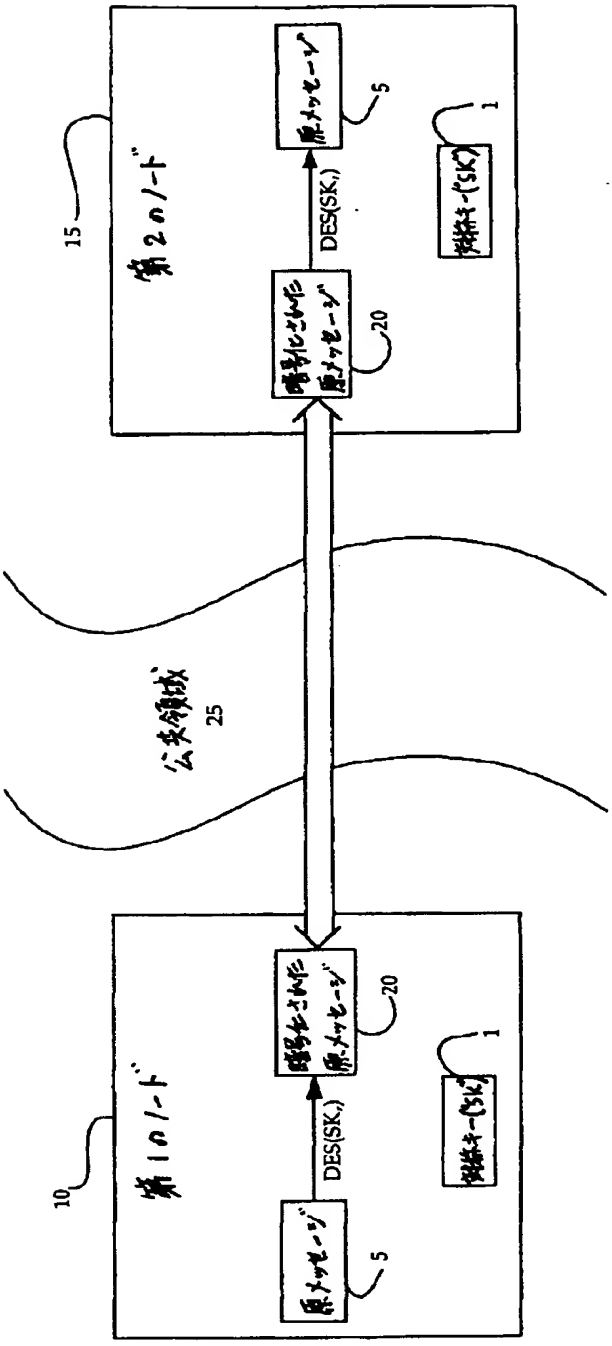

Figure 1

【 図2 】

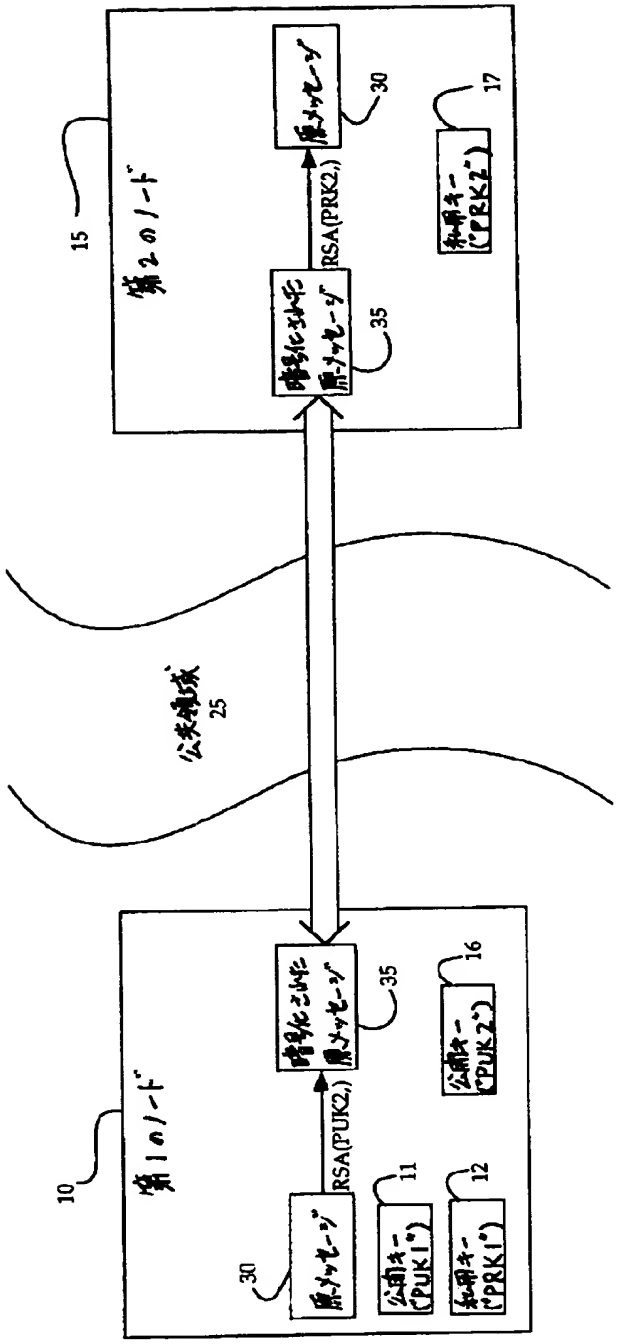
第2のノード
15
原メッセージ
30
RSA(PRK2,)
暗号化された原メッセージ
35
私用キー ("PRK2")
17
公共領域
25
第1のノード
10
暗号化された原メッセージ
35
RSA(PUK2,)
公開キー ("PUK2")
16
原メッセージ
30
公開キー ("PUK1")
11
私用キー ("PRK1")
12

Figure 2

【 図３ 】

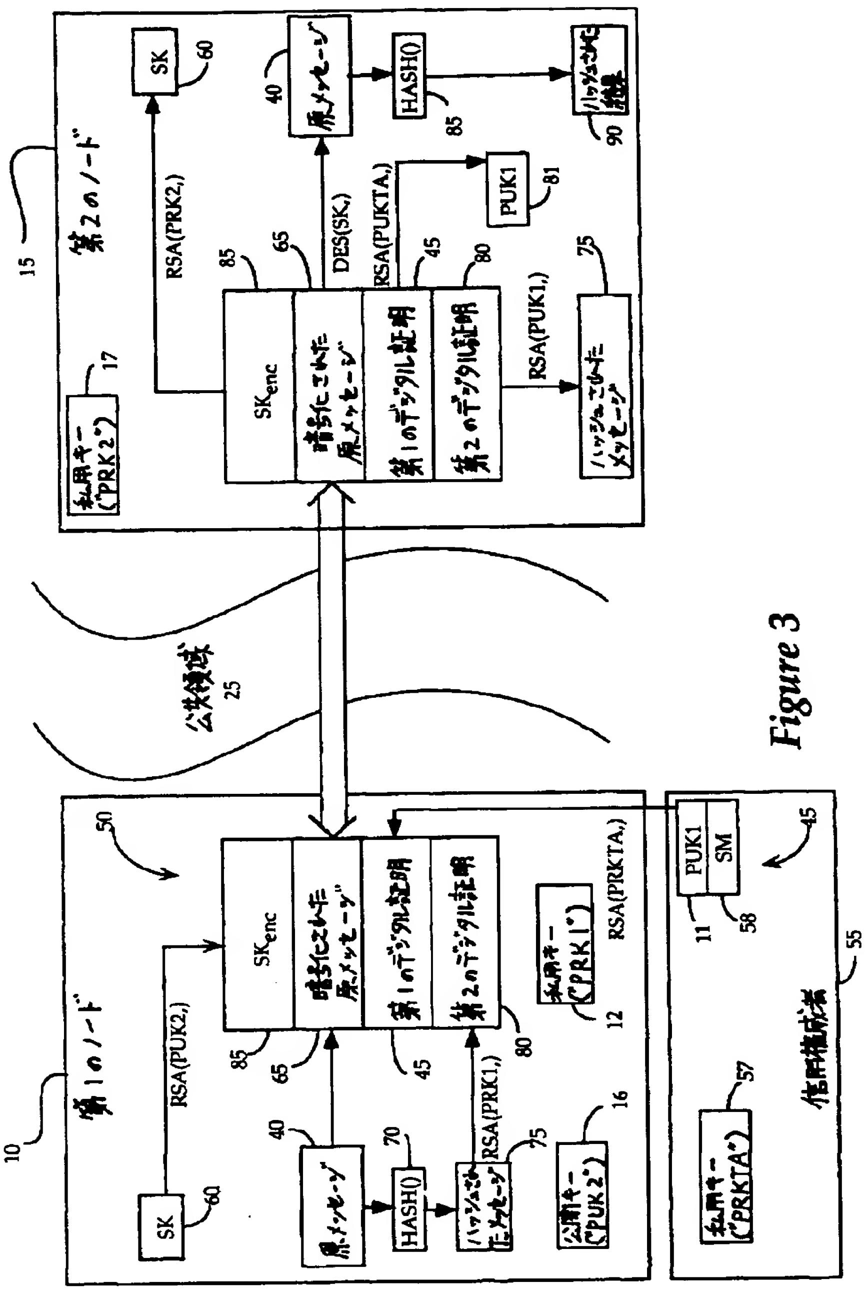
第2のノード
15
私用キー ("PRK2")
17
SK
60
RSA(PRK2,)
SK_enc
85
原メッセージ
40
DES(SK,)
暗号化された原メッセージ
65
RSA(PUKTA,)
PUK1
81
第1のデジタル証明
45
HASH()
85
第2のデジタル証明
80
RSA(PUK1,)
ハッシュされたメッセージ
75
90
公共領域
25
第1のノード
10
SK
60
RSA(PUK2,)
SK_enc
85
原メッセージ
40
HASH()
70
暗号化された原メッセージ
65
ハッシュされたメッセージ
75
RSA(PRK1,)
第1のデジタル証明
45
第2のデジタル証明
80
公用キー ("PUK2")
16
私用キー ("PRK1")
12
RSA(PRKTA,)
50
PUK1
SM
11
58
45
信用権限者
55
私用キー ("PRKTA")
57

Figure 3

【 図４ 】

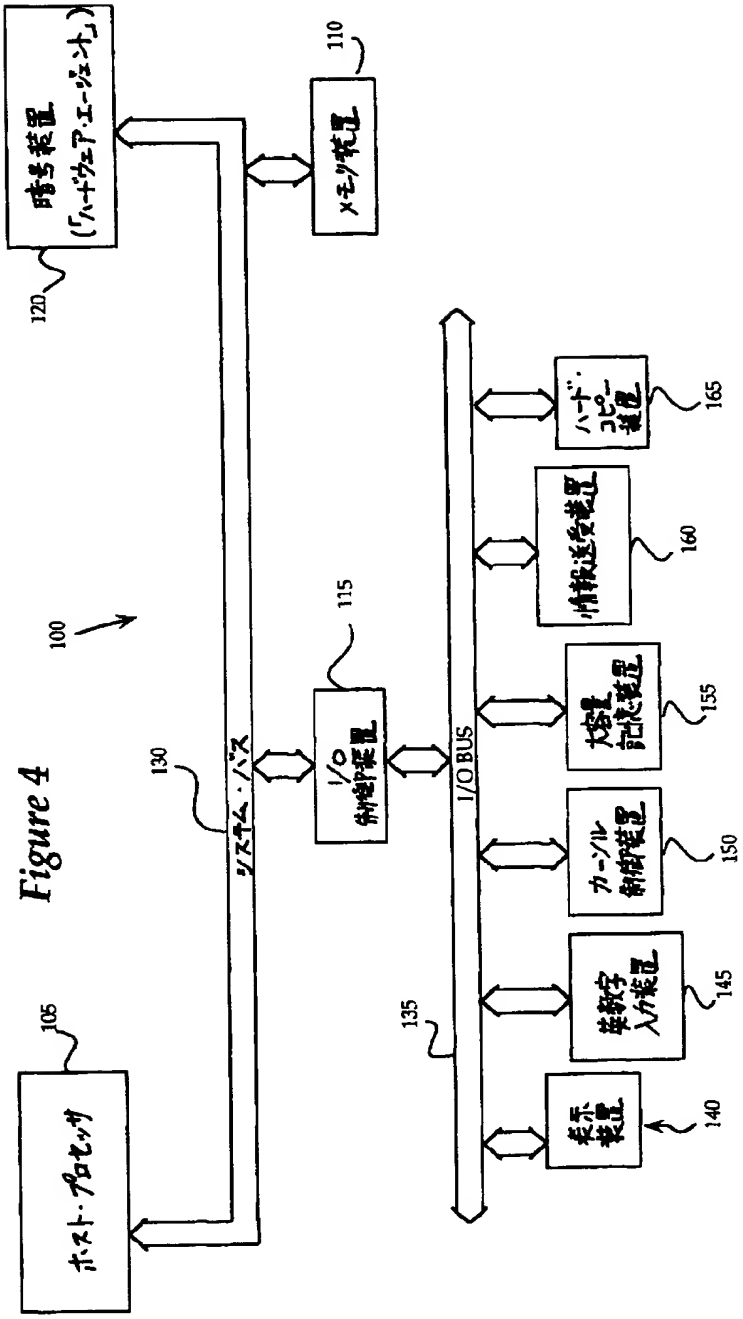
時当装置
(「ハードウェア・エージェント」)
120
110
メモリ装置
100
115
I/O 制御装置
130
システム・バス
I/O BUS
135
ホスト・プロセッサ
105
ハード・コピー装置
165
情報送受装置
160
大容量記憶装置
155
カーソル制御装置
150
英数字入力装置
145
表示装置
140

Figure 4

【 図５ 】

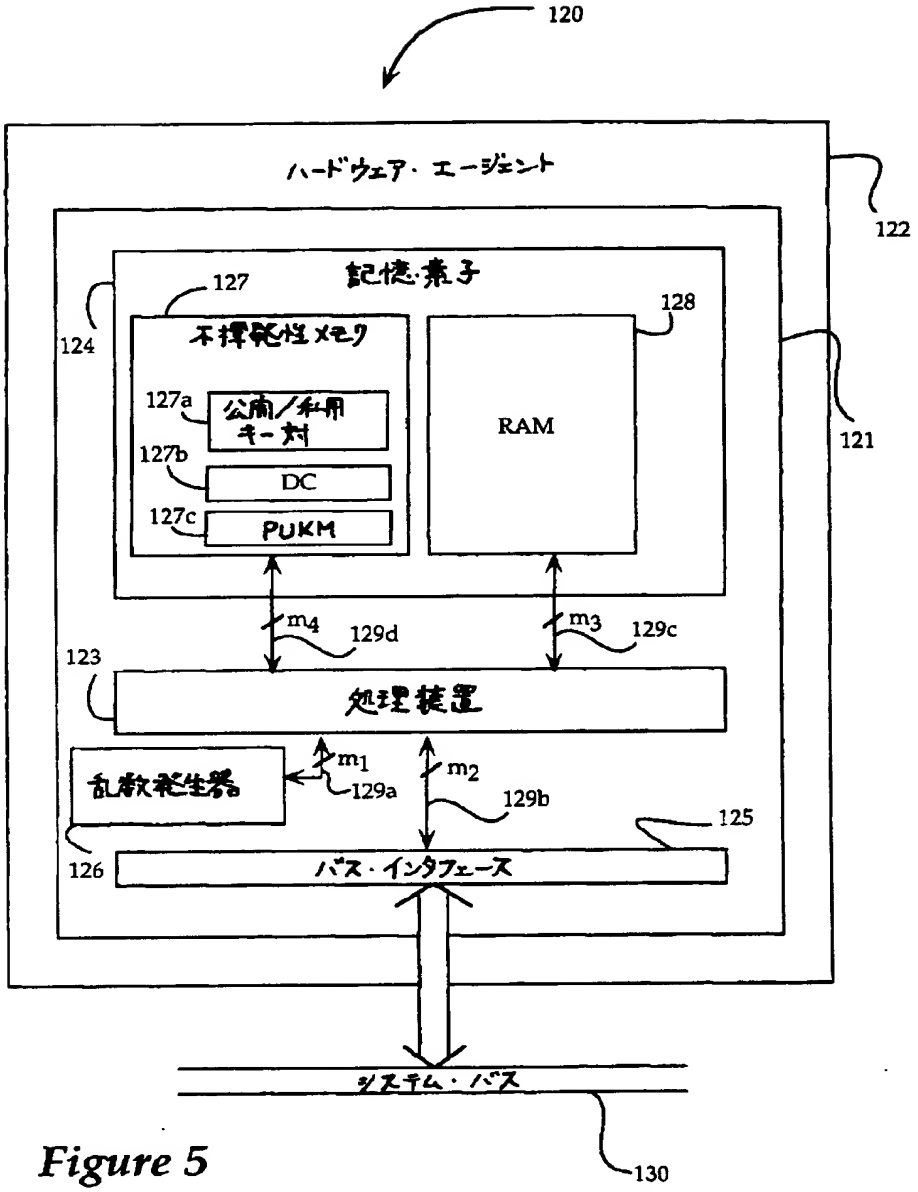
120
ハードウェア・エージェント
122
記憶素子
127
124
不揮発性メモリ
128
127a
公開/私用
キー対
RAM
121
127b
DC
127c
PUKM
m4
129d
m3
129c
123
処理装置
m1
129a
m2
129b
乱数発生器
125
126
バス・インタフェース
システム・バス
130

Figure 5

【 図6 】

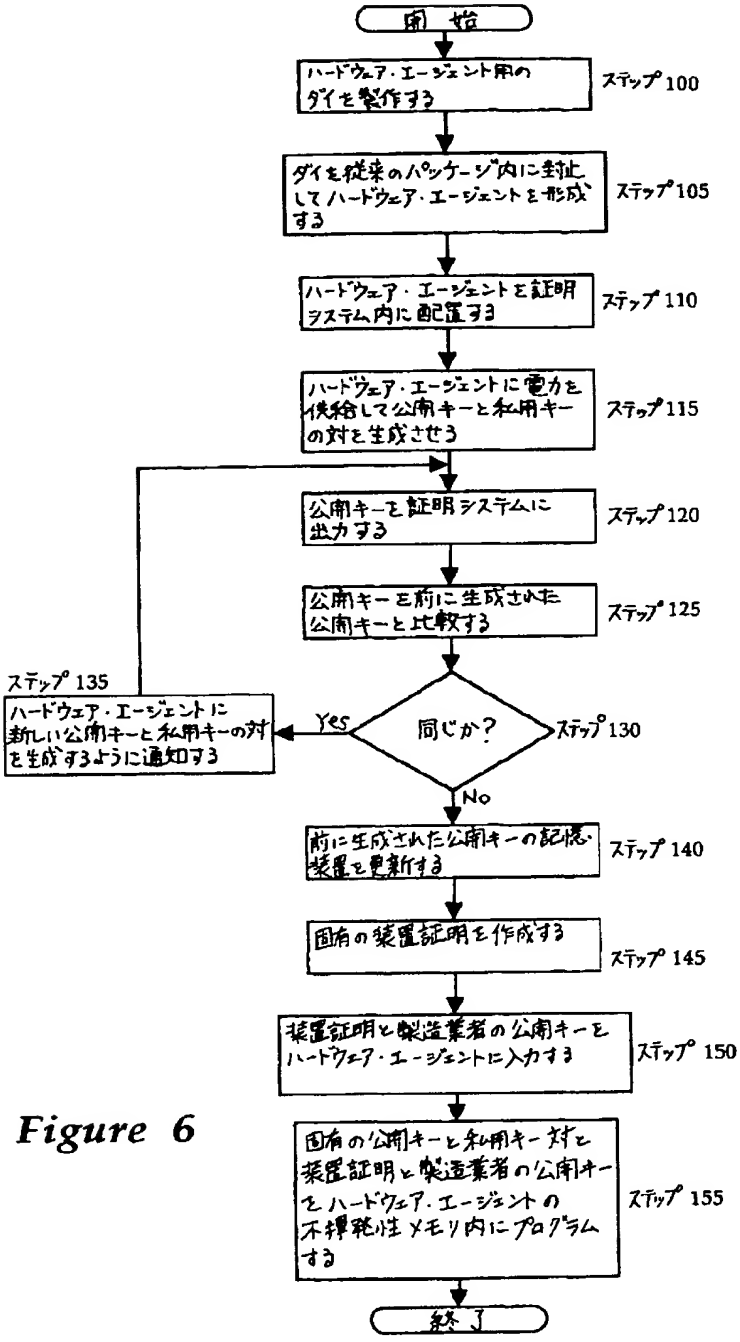
開始
ハードウェア・エージェント用のダイを製作する
ステップ100
ダイを従来のパッケージ内に封止してハードウェア・エージェントを形成する
ステップ105
ハードウェア・エージェントを証明システム内に配置する
ステップ110
ハードウェア・エージェントに電力を供給して公開キーと私用キーの対を生成させる
ステップ115
公開キーを証明システムに出力する
ステップ120
公開キーを前に生成された公開キーと比較する
ステップ125
同じか？
ステップ130
Yes
No
ステップ135
ハードウェア・エージェントに新しい公開キーと私用キーの対を生成するように通知する
前に生成された公開キーの記憶装置を更新する
ステップ140
固有の装置証明を作成する
ステップ145
装置証明と製造業者の公開キーをハードウェア・エージェントに入力する
ステップ150
固有の公開キーと私用キー対と装置証明と製造業者の公開キーをハードウェア・エージェントの不揮発性メモリ内にプログラムする
ステップ155
終了

Figure 6

【 図７ 】

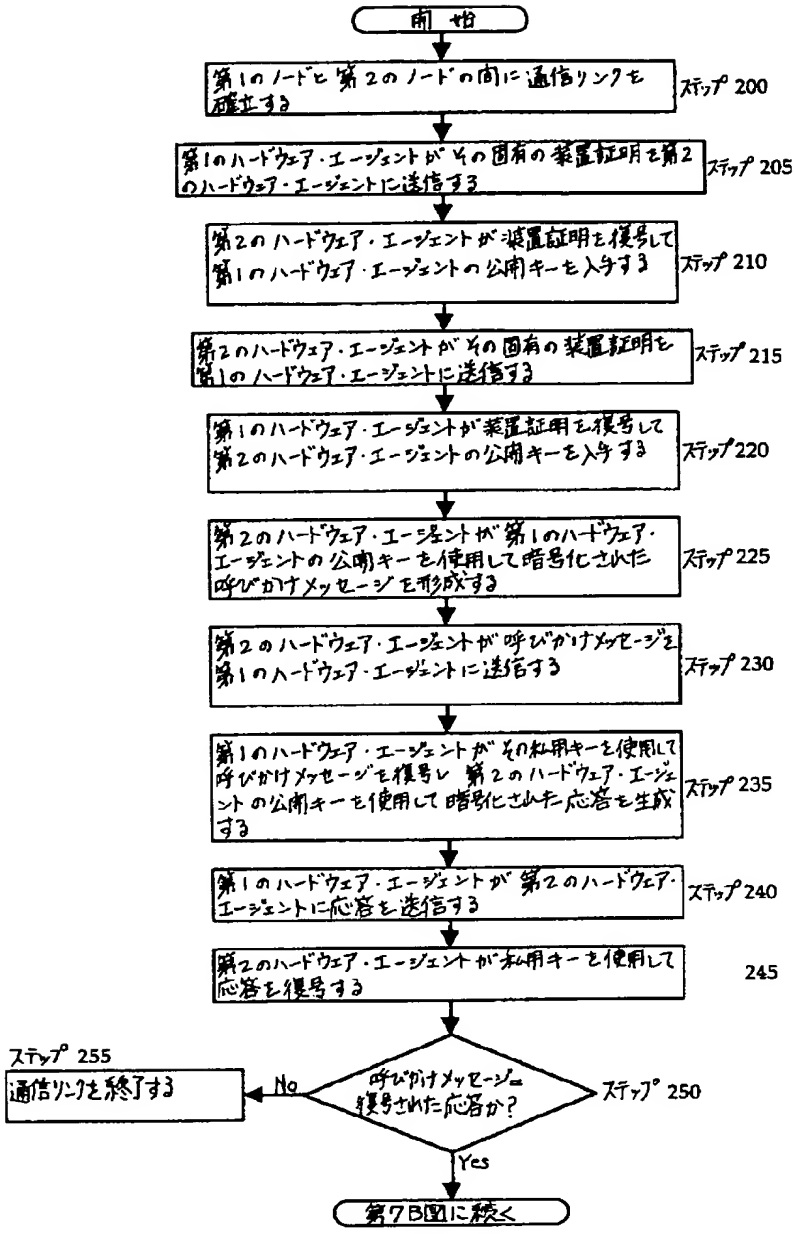
開始
第1のノードと第2のノードの間に通信リンクを確立する
ステップ 200
第1のハードウェア・エージェントがその固有の装置証明を第2のハードウェア・エージェントに送信する
ステップ 205
第2のハードウェア・エージェントが装置証明を復号して第1のハードウェア・エージェントの公開キーを入手する
ステップ 210
第2のハードウェア・エージェントがその固有の装置証明を第1のハードウェア・エージェントに送信する
ステップ 215
第1のハードウェア・エージェントが装置証明を復号して第2のハードウェア・エージェントの公開キーを入手する
ステップ 220
第2のハードウェア・エージェントが第1のハードウェア・エージェントの公開キーを使用して暗号化された呼びかけメッセージを形成する
ステップ 225
第2のハードウェア・エージェントが呼びかけメッセージを第1のハードウェア・エージェントに送信する
ステップ 230
第1のハードウェア・エージェントがその私用キーを使用して呼びかけメッセージを復号し第2のハードウェア・エージェントの公開キーを使用して暗号化された応答を生成する
ステップ 235
第1のハードウェア・エージェントが第2のハードウェア・エージェントに応答を送信する
ステップ 240
第2のハードウェア・エージェントが私用キーを使用して応答を復号する
245
呼びかけメッセージ＝復号された応答か？
ステップ 250
No
ステップ 255
通信リンクを終了する
Yes
第7B図に続く

Figure 7A

【 図7 】

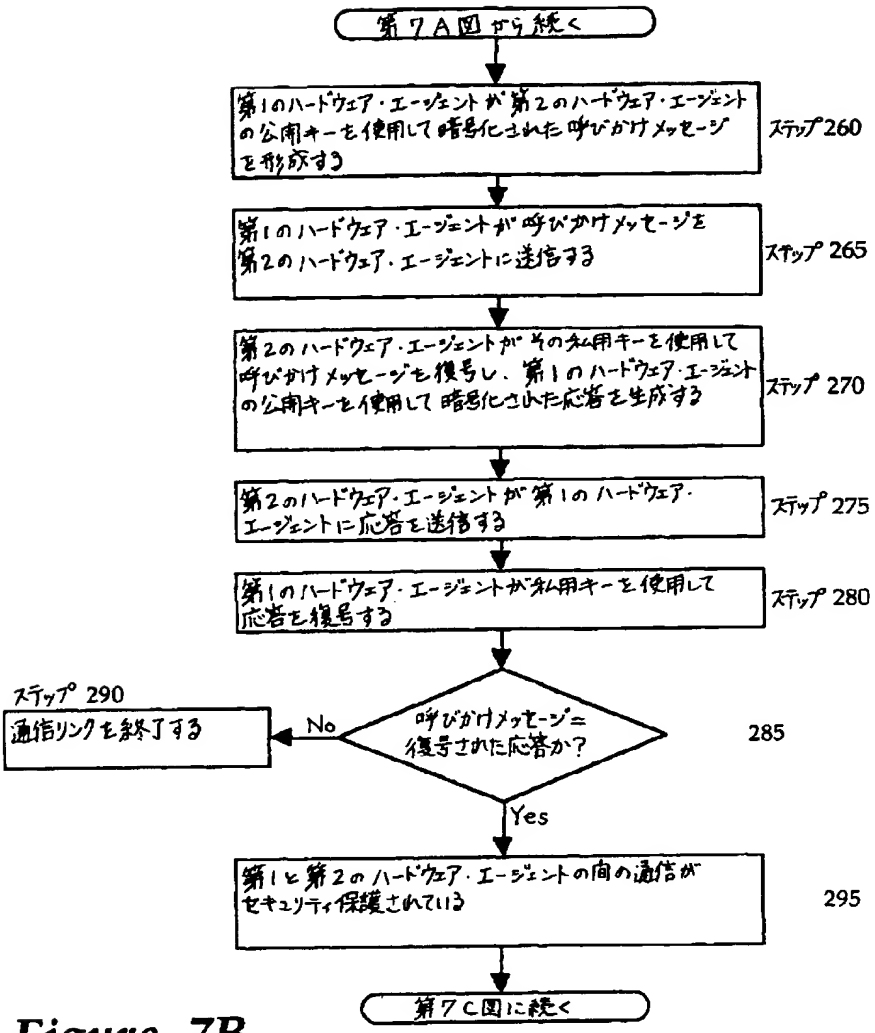
第7A図から続く
第1のハードウェア・エージェントが第2のハードウェア・エージェントの公開キーを使用して暗号化された呼びかけメッセージを形成する
ステップ260
第1のハードウェア・エージェントが呼びかけメッセージを第2のハードウェア・エージェントに送信する
ステップ265
第2のハードウェア・エージェントがその私用キーを使用して呼びかけメッセージを復号し、第1のハードウェア・エージェントの公開キーを使用して暗号化された応答を生成する
ステップ270
第2のハードウェア・エージェントが第1のハードウェア・エージェントに応答を送信する
ステップ275
第1のハードウェア・エージェントが私用キーを使用して応答を復号する
ステップ280
呼びかけメッセージ＝復号された応答か?
285
No
ステップ290
通信リンクを終了する
Yes
第1と第2のハードウェア・エージェントの間の通信がセキュリティ保護されている
295
第7C図に続く

Figure 7B

【 図7 】

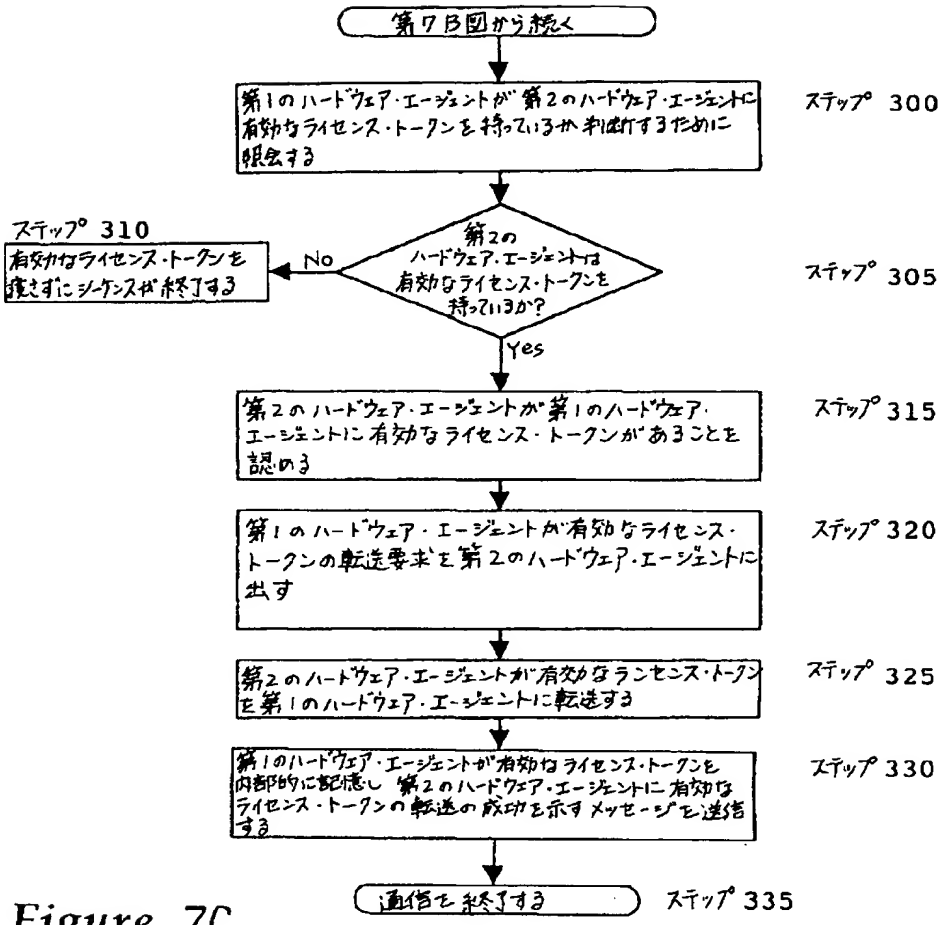
第7B図から続く
第1のハードウェア・エージェントが第2のハードウェア・エージェントに有効なライセンス・トークンを持っているか判断するために照会する
ステップ 300
第2のハードウェア・エージェントは有効なライセンス・トークンを持っているか?
No
ステップ 305
ステップ 310
有効なライセンス・トークンを得ずにシーケンスが終了する
Yes
第2のハードウェア・エージェントが第1のハードウェア・エージェントに有効なライセンス・トークンがあることを認める
ステップ 315
第1のハードウェア・エージェントが有効なライセンス・トークンの転送要求を第2のハードウェア・エージェントに出す
ステップ 320
第2のハードウェア・エージェントが有効なライセンス・トークンを第1のハードウェア・エージェントに転送する
ステップ 325
第1のハードウェア・エージェントが有効なライセンス・トークンを内部的に記憶し第2のハードウェア・エージェントに有効なライセンス・トークンの転送の成功を示すメッセージを送信する
ステップ 330
通信を終了する
ステップ 335

Figure 7C

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11136

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04K 1/00
US CL :380/25, 4, 23, 30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25, 4, 23, 24, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,807,288 (UGON, ET AL). 21 February 1989	1-20

☐ Further documents are listed in the continuation of Box C.　☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 13 DECEMBER 1995	Date of mailing of the international search report 21 FEB 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer DAVID CAIN Telephone No. (703) 306-1836

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(81)指定国　　EP (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP (KE, MW, SD, SZ, UG), AM, AT, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, CZ, DE, DE, DK, DK, EE, ES, FI, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK, TJ, TM, TT, UA, UG, UZ, VN